October 18, 2001

Bill Bell
Project Manager
Consolidated Customer Service System
Bank of California Building
Seattle, Washington 98104

Dear Mr. Bell:

Attached is our audit report regarding the Consolidated Customer Service System (CCSS). We conducted this audit to evaluate the adequacy of the information technology security controls over CCSS. Overall, we found that the controls over CCSS were generally adequate; however, our report contains recommendations that we believe will improve the system's security.

We solicited comments from your office on our draft audit findings, and have included these comments in this published report. We appreciate the assistance and cooperation provided by CCSS officials during our audit.

Linneth Riley-Hall, Assistant City Auditor, was the auditor-in-charge for this project. Consultant Jack Champlain assisted her during the audit. Please call Linneth (206-233-0088) or the Deputy City Auditor, David Jones (206-233-1095), if you have any questions regarding this work.

Sincerely,

Susan Cohen
City Auditor

Enclosure

cc: Jan Drago, Chair, Finance, Budget and Economic Development Committee
Jim Compton, Chair, Public Safety and Technology Committee
Ruth Riddle, State Auditor's Office

AUDIT PURPOSE

The Office of City Auditor conducted this audit to evaluate the effectiveness of the information technology security controls established for the City of Seattle's Consolidated Customer Service System (CCSS).

PROJECT HISTORY

CCSS was designed to replace the City of Seattle's two utility billing systems: CIS (Customer Information Systems) and CUBS (Combined Utility Billing System). The City of Seattle issued the original request for proposal for CCSS in the summer of 1997. In January 1998 the City of Seattle selected the BANNER system from Systems & Computer Technology Corporation Utility Systems, Inc. (SCT) of Columbia, South Carolina. The software contracts and license agreements were finalized in June 1998. In January 1999 the project completion cost was estimated at $18 to $20 million. The new system was projected to save the City approximately $1.6 million in annual operating costs. Implementation was set for February 2000. By September 1999 the estimated cost to complete the project had increased to $26 million, and project implementation was rescheduled to May 2000. As of February 2001, the revised cost estimate had risen to a total of $40.2 million. The project was implemented April 2, 2001.

AUDIT OVERVIEW

The audit originally began in July 1999. However, soon after beginning our audit work, it became evident that the project would not be completed in February 2000 as originally planned. Therefore, we decided to suspend the audit in September 1999. The audit recommenced in March 2000 in anticipation of the revised CCSS implementation date of May 1, 2000. Due to additional project delays, we opted to suspend the audit again. The audit recommenced in January 2001 and our testing was completed on March 27, 2001.

AUDIT METHODOLOGY

Our audit methodology consisted of interviews, observations, and detailed audit tests conducted during individual and group meetings with personnel from the CCSS project and the City of Seattle's computer center. We tested CCSS's information technology security controls against a set of general information technology security standards, which we considered reasonable given the intended uses of the CCSS system and the associated risks. We did not examine controls over the CCSS network server located in the Bank of California Building, nor did we assess business resumption controls in the CCSS business units.

AUDIT CONCLUSION

We considered the information technology security controls over the CCSS system to be generally adequate. However, we identified eight internal control concerns that are documented as discussion points in the detailed results section, and also made recommendations to assist CCSS management in resolving the concerns.

Detailed Results of Audit

Audit Step 1: Physical security controls

Physical security controls help ensure that programs and data on the CCSS application, database servers and storage devices are not copied, deleted, altered, or otherwise accessed by unauthorized persons. They also help ensure timely recovery in the event of earthquakes, fires, floods, and other natural and man-made disasters.

On January 31, 2001, we assessed the adequacy of physical security over the CCSS system hardware located in the City's computer center. We did not identify any significant physical security control weaknesses. We observed the following controls: around the clock security guard service, electronic access badge door locks, halon gas fire suppression system, water detection system, fire extinguishers, surveillance cameras, uninterruptible power supply (UPS) battery system with 15 minutes of graceful shutdown power, two electric power feeds, recovery controls internal to the IBM S85 central processing unit (CPU) and supporting data storage devices. These devices enable immediate data recovery upon restoration of power and produce daily data backups which are stored at a secure offsite location. At the time of this review the City was in the process of finalizing negotiations on a two-year contract with Sunguard, Inc. to provide a hot site data center in Philadelphia, Pennsylvania in the event of a disaster in Seattle. We did not identify any significant physical security control weaknesses.

Conclusion: The physical security controls over the CCSS hardware located at the City's computer center were adequate. We found that the CCSS S85 CPU was not connected to the UPS system due to capacity limitations. Computer center management stated that this situation would be resolved when the center moves to the Key Tower in November 2001. Therefore, we did not believe recommendations for control improvement were necessary.

Audit Step 2: System access controls

To help ensure that users were not granted system access capabilities that could enable them to perform unauthorized transactions or functions not required for their normal duties, or damage the functionality of the system we: (a) assessed whether adequate logical segregation of duties could be achieved while preserving operational effectiveness; and (b) observed a test audit user-ID being created and assigned selected access capabilities.

We examined CCSS (i.e., SCT BANNER 2000) application security documentation and found that BANNER, with the use of its role-level security features, could adequately segregate user access capabilities. On March 27, 2001, we observed the CCSS Security Administrator logon and create a test user-ID. As part of the setup, we required the SA to assign various access roles. The SA stated that user access could be further limited to no access, read-only and update, and could be restricted to Seattle City Light and/or Seattle Public Utilities information, but we did not test these capabilities. As of March 27, 2001, there were reportedly over 600 CCSS users.

Conclusion: CCSS contained adequate controls to segregate duties once it entered production. However, we noted the following internal control concerns.

Discussion Point 1: We had planned to assess the reasonableness of the access capabilities assigned to a judgmental sample of CCSS users, especially those with SA and database administrator (DBA) capabilities. However, since the CCSS system had not yet gone live at the time of our field work, we could not perform detailed testing of individual system access

capabilities. At that time, there were reportedly still many developers with SA and/or DBA access.

Recommendation 1: We recommend that CCSS management implement procedures, whereby the CCSS SAs prepare lists of users and their access capabilities by department on an annual or more frequent basis. The lists should be sent to department managers for review and approval. The SAs should archive the approved lists until the subsequent review has been completed. We further recommend that the maiden review be performed within six months of the CCSS implementation (e.g., October 2001).

CCSS Management Response:

We have implemented this recommendation. The initial listing was sent out to user supervisors on July 27th and we have received feedback from the supervisors. The changes have been posted to the BANNER Security Tables. This process is scheduled to take place every two months.

Discussion Point 2*:* At the time of our audit, CCSS had not developed formal written SA procedures for adding, changing and deleting CCSS users.

Recommendation 2: We recommend that written SA procedures be developed. Such procedures should include the following controls:

A. SAs should obtain management authorization via email and/or a special CCSS User Access Request Form before adding, changing or deleting user access capabilities.

B. SAs should have the authority to temporarily veto a manager's request to assign role levels, which could cause inadequate segregation of duties, until the request can be considered by the appropriate higher level of management.

C. SAs should delete users from CCSS in a timely manner when their job functions change due to transfers, promotions, demotions or terminations. CCSS management should work with the City's Personnel Department and other human resource officials to develop a Citywide procedure for notifying CCSS security when personnel changes are made that affect an employee's CCSS privileges.

CCSS Management Response:

The procedures were documented and implemented when CCSS went "live". Subsequently, we provided the following procedures for your review: "Obtaining Access to CCSS BANNER and Bill View", "Providing Access to CCSS BANNER and Bill View Internal Procedure", "Form", "Supplemental Page", "Resetting Passwords" and "Obtaining Access to Other CCSS Databases".

Audit Step 3: Security parameter settings

To help ensure that unauthorized access to CCSS is prevented through the deployment of strong password security controls and secured audit logs, we documented and assessed the reasonableness of CCSS security parameter settings.

On March 27, 2001, we observed the CCSS SA logon, create a test audit user-ID, and perform various password control tests under our direction.

Conclusion: CCSS password security controls and audit logging capabilities should be improved, thereby significantly decreasing the risk of unauthorized access.

Discussion Point 3: We identified nine areas in which CCSS would benefit from improved security parameter settings.

Recommendation 3: We recommend that CCSS management work with SCT to develop and implement adequate security parameter controls.

CCSS Management Response:

We have requested that the vendor, SCT, consider expanding BANNER's security in a future release of the BANNER product. SCT has taken this under advisement at this time.

Audit Step 4: Logical security controls

We tested existing logical security controls of the CCSS system (e.g., password masking, minimum password length, invalid password attempts) to ensure they were functioning properly.

On March 27, 2001, we observed the CCSS SA logon, create a test audit user-ID, and perform various password control tests under our direction. We observed the following controls: passwords were masked as *'s on the screen when typed by the SA; a blank password was rejected; and after three failed logon attempts the SA's user-ID was returned to the desktop.

Conclusion: The logical security controls listed above functioned properly, but need improvement. Because the recommendations to resolve these logical security control weaknesses were already documented in Audit Step 3, we did not believe additional recommendations for internal control improvement were necessary.

Audit Step 5: Password file and job script controls

To help ensure that unauthorized access to CCSS cannot be gained by anyone who has access to the password file, we assessed whether the file containing user passwords was encrypted and could not be viewed by anyone, including a SA or DBA. We also assessed whether passwords of superuser-IDs were hard coded into job scripts.

On March 27, 2001, we asked a SCT Technical Consultant about password file encryption. He stated that the password file was encrypted within the Oracle database management system (DBMS) and could not be viewed in clear text by SAs or DBAs. This response was consistent with what we learned during our 1999 audit of the City's Summit System, and with our knowledge of the Oracle DBMS.

We also asked the SCT official whether AIX operating system (OS) superuser-IDs and passwords were hard coded into any job scripts. He stated that OS superuser-IDs and passwords were not, but that SCT BANNER superuser-IDs and passwords were hard coded into some job scripts.

Conclusion: The password file was adequately encrypted. However, we identified the following internal control concern.

Discussion Point 4: Since SCT BANNER superuser-IDs and passwords were hard coded into some job scripts, the possibility exists that users with access to the job scripts (i.e., AIX SAs,

Oracle DBAs and some developers) could find the superuser-IDs and passwords, and then gain unauthorized superuser access to CCSS. The existing practice also requires each script to be updated whenever the password changes. For example, if a 60-day password change requirement is implemented for all CCSS user-IDs, then all scripts containing passwords will need to be manually updated at least every 60 days. If any scripts are missed, the associated production jobs will fail.

Recommendation 4: We recommend that CCSS management work with SCT to program BANNER superuser-ID password variables into the affected job scripts. This will enable the passwords to be administered in one or a few locations, and allow timely changing of the passwords on a periodic basis.

CCSS Management Response:

We have taken this recommendation under advisement and are currently working on a solution to this issue. The solution is scheduled to be completed during the fourth quarter of 2001; however, implementation of this may need to be delayed until the first quarter of 2002.

Audit Step 6: Logging of security events

To help ensure that system problems recorded in the audit log (as determined by the parameters examined in Audit Step 3) are being reviewed to the extent necessary to detect unauthorized activities in a timely manner, we assessed the adequacy of procedures to review any logged system security related events (e.g., failed logon attempts, when passwords are changed, when users are added or deleted, when user access capabilities are changed, when system security parameters are changed, attempted changes to the audit log and system restarts, etc.).

On March 27, 2001, we asked the SA about procedures for reviewing logged events. As documented in Discussion Point 3, CCSS's controls related to logging of security related events need improvement. The main events that would appear in the existing audit log would be failed access attempts to various objects[1] due to unauthorized changes to the three SEED numbers which are critical to the encryption and authentication processes for SQL*Forms, COBOL, and C. The SA stated that she could review the audit log on a regular basis.

Conclusion: At the time of our audit, CCSS's procedures to review the audit log on a daily basis were not adequate. We identified the following internal control concern.

Discussion Point 5: CCSS had not developed documented procedures concerning the review of the BANNER audit log, including escalation procedures in the event of suspicious activities.

Recommendation 5: Upon creation of improved password security and logging controls as documented in Recommendation 3, CCSS management should document and implement procedures for the logs to be reviewed. The procedures should specify which events to log, who should review the logs and how often, and the period for which the logs will be retained and archived (e.g., one year). If practical, the logs should be written to a protected environment (e.g., optical disk in an area where CCSS SAs, DBAs, and AIX SAs do not have access; we recognize that this could be an expensive solution).

[1] An object is an independent software program module containing data that is written in an object-oriented programming language.

CCSS Management Response:

The Base BANNER Security Maintenance Package includes a security violation log for System Administrators to monitor. It shows the security violation, user, date, time and level of violation. Our operation's procedure calls for this security log to be reviewed by the Security Administrator each week on Friday.

Audit Step 7: Software and security quality assurance process

We sought to verify that the CCSS project had an established process to identify, monitor and resolve software problems that could compromise the effectiveness of the system's security.

We examined CCSS project documentation pertaining to goals and deliverables from 1999 to the present. Key documents included project goals and performance standards from September 1999, an April 2000 draft security plan, and February 2001 steering committee minutes.

Conclusion: The CCSS project had an effective process to monitor and resolve project software problems. However, we identified the following internal control concern.

Discussion Point 6: CCSS project goals and performance standards did not provide for adequate security controls, as evidenced by the various discussion points within this audit report.

Recommendation 6: We recommend that the City require that the types of physical and logical security controls described in this report are integrated into the City's information technology project management process to ensure that future projects include them as required deliverables (e.g., password set-up requirements).

CCSS Management Response

We concur with your recommendation; however, this is beyond the scope of the CCSS Project and we suggest that this recommendation be directed to Marty Chakoian, the Chief Technology Officer at the Department of Information Technology. No action is planned on the part of the CCSS Team.

Audit Step 8: Default password

To help ensure that unauthorized access to CCSS cannot be gained by signing on as the initial SA using the original default superuser password, we determined whether the original default SA password had been changed, controls existed to change it on a periodic basis (e.g., quarterly), and whether the current password was known by multiple SAs and/or DBAs.

On March 27, 2001, we observed an SA's attempt to logon using both user-IDs with the default password. Both attempts failed, proving that the default password had been changed.

Conclusion: The passwords of the initial SA user-IDs were changed. However, we identified the following internal control concern.

Discussion Point 7: Since the CCSS system was not in production at the time of our test, there were no controls in place to ensure that the superuser-ID passwords were changed on a regular basis. We do not know how many people currently know the password.

Recommendation 7: Upon successful CCSS production implementation, we recommend that the superuser-ID passwords be changed, that the passwords be known only by designated SAs, DBAs and their backups, and that procedures be implemented to change these passwords every 60 days or more often when necessary (e.g., when a SA terminates).

CCSS Management Response:

We have taken this recommendation under advisement and are currently working on a solution to this issue. The solution is scheduled to be completed during the fourth quarter of 2001, however, implementation of this may need to be delayed until the first quarter of 2002.

Audit Step 9: Written security procedures

To help ensure that system security related controls are deployed by SAs, DBAs, and CCSS management in an effective and timely manner, we planned to assess the adequacy of written system security procedures.

Conclusion: At the time of our audit, CCSS had not developed and issued a comprehensive set of written security procedures. We considered the absence of such documents to be an internal control concern.

Discussion Point 8: At the time of our review, CCSS had not developed and issued a comprehensive set of written system security procedures for the project.

Recommendation 8: We recommend that, upon creation of improved security controls as documented in Recommendations 3 and 5, CCSS management develop a comprehensive set of CCSS security procedures. The security procedures should clearly explain the security responsibilities of the CCSS SAs versus those delegated to the departments. For example, they should state the following:

1) Departments should inform CCSS SAs immediately when one of their employees is terminated, transferred, or demoted so that SAs can make the necessary security changes.

2) SAs should periodically provide department managers with a list of users that report to the managers and the CCSS access capabilities of each user. CCSS should require that the managers review the access capabilities of each user in their departments, and certify in writing whether the capabilities are necessary for the users to perform their normal duties. This certification should be performed at least annually, or more often if deemed necessary by senior management.

3) The procedures should list the specific actions that should be performed by SAs in the event of an unauthorized intrusion or internal security breach of CCSS. These procedures should specify under what conditions the intrusion or breach should be escalated to senior management.

CCSS Management Response:

The procedures were documented and implemented when CCSS went "live". We have provided you with the procedure for your review – "Maintaining CCSS BANNER."